

# Two-sided Quantum Amplitude Amplification and Exact-Error Algorithms

Debajyoti Bera \*

May 9, 2016

## Abstract

Amplitude amplification is a central tool used in Grover's quantum search algorithm and has been used in various forms in numerous quantum algorithms since then. It has been shown to completely eliminate one-sided error of quantum search algorithms where input is accessed in the form of black-box queries. We generalize amplitude amplification for two-sided error quantum algorithm for decision problems in the familiar form where input is accessed in the form of initial states of quantum circuits and where arbitrary projective measurements may be used to ascertain success or failure. This generalization allows us to derive interesting applications of amplitude amplification for distinguishing between two given distributions based on their samples, detection of faults in quantum circuits and eliminating error of one and two-sided quantum algorithms with exact errors.

## 1 Introduction

The motivation behind this work is to investigate the characteristics of quantum computation when viewed as randomized algorithms. It is known that quantum amplitude amplification, the key technique underlying Grover's unordered search algorithm, is able to reduce and even eliminate error of one-sided quantum black-box algorithms for search problems [7]. We explored that direction further for two-sided error algorithms for decision problems based on the key observation that quantum algorithms appear to be better at distinguishing between two given probability distributions compared to classical randomized algorithms.

Suppose we are given a biased coin whose distribution is either  $\mu_1 = \langle 1/3, 2/3 \rangle$  or  $\mu_2 = \langle 2/3, 1/3 \rangle$ . A classical problem of probabilistic classification is to determine the distribution of the coin by tossing it several times. Various techniques exist like Bayesian classification and maximum likelihood estimation, all of which aim to minimize some kind of error that is inherent in such a probabilistic inference. But it is not believed to be possible to confidently classify a distribution without any error. This is true even if  $\mu_1 = \langle 0, 1 \rangle$  instead.

However, such classification is possible when the distributions come from a *quantum system*, our definition of a quantum source of random samples. We define a quantum system (QS) as a combination of a quantum circuit  $C$ , an input to the circuit  $|\psi\rangle$  and a two-outcome projective measurement operator  $\mathcal{P} = \langle P_E, I - P_E \rangle$  (two outcomes will be *always labeled as E and F* for convenience) and denote it by  $\langle |\psi\rangle, C, \mathcal{P} \rangle$ . If we are given an actual instance of a QS and we *apply the circuit on the input followed by measurement using the projective operator*, we will obtain a sample in  $\{E, F\}$  from the output probability distribution  $\langle p_E, 1 - p_E \rangle$  where  $p_E$  denotes the probability of observing outcome  $E$  when  $C|\psi\rangle$  is measured using  $\mathcal{P}$ .

The quantum version of the above question of classifying between  $\mu_1$  and  $\mu_2$  becomes this: given an instance  $Q$  which can be either a quantum system  $Q_1$  with output distribution  $\mu_1$  or QS  $Q_2$  with output distribution  $\mu_2$ , can we confidently figure out if  $Q$  is  $Q_1$  or  $Q_2$  (in other words, determine the actual distribution of  $Q$ ) by using  $Q$  in a black-box manner? Assume that both  $Q_1$  and  $Q_2$  involve the same number of qubits and the same set of outcomes ( $E$  and  $F$ ). This is analogous to asking if two or more distinct distributions (over same support of two elements) can be distinguished without any probability of error. Even though classical techniques cannot identify the exact distribution from the

---

\*IIIT-Delhi, New Delhi, India. Email: [dbera@iiitd.ac.in](mailto:dbera@iiitd.ac.in)

sample distribution without any error, we show that it is possible to do so for distributions of quantum systems.

**Theorem 1.** *Given a quantum system  $\mathcal{Q} = \langle |\psi\rangle, C, \mathcal{P} \rangle$  whose output distribution can either be  $\langle \delta, 1 - \delta \rangle$  or  $\langle \epsilon, 1 - \epsilon \rangle$  for some  $0 \leq \delta < \epsilon \leq 1$ , there is a quantum circuit  $C'$  which can determine the output distribution of  $\mathcal{Q}$  without any probability of error.  $C'$  takes  $|\psi\rangle$  as input, makes repeated calls to  $C$ ,  $C^\dagger$  and employs gates that depend upon operators of  $\mathcal{P}$  and  $|\psi\rangle$ .*

The core technique is once again, *quantum amplitude amplification*. It can be thought of as a quantum analog of repeated trials used in randomized algorithms for reducing mis-classification error. It is the workhorse behind Grover's famous quantum unordered search algorithm [8] and was later shown to be also applicable to the Deutsch-Jozsa problem [3]. It appears that quantum algorithm designers simply cannot wave it enough; it is applicable to almost any search problem to yield a surprising improvement, usually quadratic, over classical algorithms. Since its inception, amplitude amplification have been used, either directly or in the form of Grover's search algorithm for a vast range of problems like minimum of an unordered array [6], minimum spanning tree [5] and even clustering [1]. Nevertheless, we feel that the technique still has a long way to go, especially, when used in a non-blackbox manner.

The most generalized and popular version of this technique was given by Brassard et al.

**Theorem 2** (Exact amplitude amplification [7]). *Consider a Boolean function  $\Phi : X \rightarrow \{0, 1\}$  that partitions a set  $X$  between its good (those which  $\Phi$  evaluates to 1) and bad (those which evaluate to 0) elements. Consider also a quantum algorithm that uses no measurements and uses oracle gates for computing  $\Phi$  such that  $C|0\rangle$  is quantum superposition of the elements of  $X$  and let  $a > 0$  denote the success probability that a good element is observed if  $C|0\rangle$  is measured (in the standard basis). There exists a quantum circuit (that depends upon  $a$ ) which finds a good solution with certainty using at most  $\Theta(1/\sqrt{a})$  applications of  $C$  and  $C^\dagger$ .*

This theorem is highly versatile as it is. However, for our applications we require further generalizations. For example, we are interested in not only one-sided, but also two-sided error algorithms. We also want to apply it to algorithms which are measured not necessarily in the standard basis. Lastly, we want algorithms which act on non- $|0\rangle$  input states, specifically, input states that correspond to the input  $\Phi$ , suitably encoded – this is similar to classical Boolean circuits without oracle gates. Lastly, for the results of this paper we stick to only decision versions of the above theorem (though our results could be extended to circuits that output some solution). The following theorem is our version of Theorem 2 with the constraint that the probability  $a$  is fixed for every possible  $\Phi$  (condition of *exactness*).

**Theorem 3** (Decision version of generalized exact amplitude amplification). *Consider a Boolean function  $\Phi : X \rightarrow \{0, 1\}$  that partitions a set  $X$  between its good (those which  $\Phi$  evaluates to 1) and bad (the rest of  $X$ ) elements. Suppose  $C$  is a quantum algorithm (or circuit) that uses no measurement and decides  $\Phi$  with two-sided exact error  $(\delta, \epsilon)$  for some  $\delta < \epsilon$ . That is, the probability of error when  $C$  is given a good  $x \in X$  is exactly  $\epsilon$  and when  $x$  is bad is exactly  $\delta$ . Here success and error is determined upon measurement of the output state of  $C$  by any projective measurement with two outcomes. There exists a quantum circuit  $C'$  that calls  $C$  and  $C^\dagger$ , uses the same input as that of  $C$  (maybe with ancillae), is measured using an extension of the measurement operator for  $C$  and decides  $\Phi$  with certainty,*

The primary contribution of this paper are a few interesting applications of amplitude amplification. If we have two quantum systems which differ only in their circuit, then we can essentially use their output distribution, after suitably amplifying the systems, to distinguish between those circuits. We show how this can be used to detect faults in quantum circuits.

On the other hand, if we have two systems that differ only in their input states, then we get a way to amplify their probability of acceptance. This is exactly at the core of our proof that quantum classes equivalent to exact two-sided and exact one-sided error classes can be “derandomized”, in the sense that their errors can be completely eliminated.

One of the major, and still open, questions of *Complexity Theory* is how  $\mathbf{P}$  compares to  $\mathbf{RP}$  and  $\mathbf{BPP}$ , one-sided and two-sided bounded error polynomial-time complexity classes. The current best results are the obvious inclusions  $\mathbf{P} \subseteq \mathbf{RP} \subseteq \mathbf{BPP}$ , though there are some evidences of their equivalence. Same question for their quantum analogs is in an equally indeterminate state, i.e.,  $\mathbf{EQP} \subseteq \mathbf{RQP} \subseteq \mathbf{BQP}$ ; these are quantum analogs of  $\mathbf{P}$ ,  $\mathbf{RP}$  and  $\mathbf{BPP}$ , respectively. There is not even much evidence that

**EQP = BQP.** One approach towards settling this question is studying restricted versions of these classes. Our results show that their exact error versions, **ERQP** and **EBQP**, are identical to **EQP** as long as the two(one)-sided errors are fixed for all instances <sup>1</sup>.

**Organization:** The rest of the paper is organized as follows. We discuss quantum distinguishability of quantum systems in Section 2. The proof of our main theorem on distinguishability is given in Section 3. This theorem, even though quite general, is not suitable enough to amplify a collection of quantum systems in a uniform manner; in Section 4 we discuss a uniform version of our main theorem. Section 5 contains one of the applications about detection of faults in quantum circuits and in Section 6 we show that **EBQP** = **ERQP** = **EQP** and prove Theorem 3 for regular circuits and those with oracle gates.

## 2 Distinguishing quantum systems

We will use  $\mu_p$  to denote a distribution  $\langle p, 1 - p \rangle$  over outcomes  $\langle E, F \rangle$  and  $\mu(Q)$  to denote output distribution of a quantum system  $Q$ .

As explained earlier, the main problem we are interested in involves a given instance of a quantum system  $Q$  which can be either  $Q_\delta$  with output distribution  $\mu_\delta = \langle \delta, 1 - \delta \rangle$  or  $Q_\epsilon$  with output distribution  $\mu_\epsilon = \langle \epsilon, 1 - \epsilon \rangle$ . We want to construct a quantum algorithm, rather a circuit, that can “call  $Q$  as a subroutine” and determine if  $Q = Q_\delta$  or  $Q = Q_\epsilon$ .

We can even extend this to multiple quantum systems  $\mathcal{S} = \{Q_1, Q_2, \dots\}$  where output distribution of any  $Q_i$  is either  $\mu_\delta$  or  $\mu_\epsilon$ . We use the notation  $QD(Q_1, Q_2, \dots)$  or even shorter  $QD(\mathcal{S})$  to refer to the *quantum distinguishability* problem among quantum systems of  $\mathcal{S}$ .

Our goal is to design a quantum circuit in which we can “embed any given  $Q$ ” as a black-box. This motivated us to define a notion of black-box extension for quantum systems, similar to quantum algorithms with subroutines or quantum circuits with black-box operators, allowing only trivial extensions to inputs states and projection operators. We refer to these as  $\mathcal{B}$ -transforms ( $\mathcal{B}$  standing for “black-box”). A general illustration is given in Figure 1.

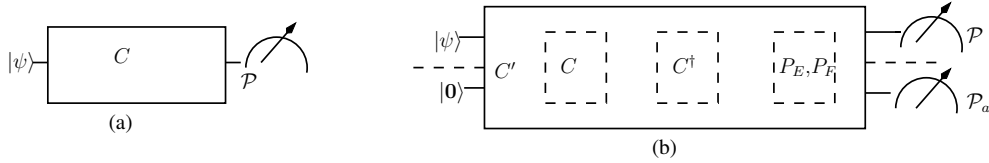


Figure 1: Schematic for  $\mathcal{B}$ -transform

**Definition 1** ( $\mathcal{B}$ -transform). A (non-uniform)  $\mathcal{B}_{\delta, \epsilon}^n$ -transform for  $n$ -qubit systems is a (non-uniform) procedure for extending an  $n$ -qubit QS  $Q_1 = \langle |\psi\rangle, C, P \rangle$  to a (possibly larger) QS  $Q_2 = \langle |\psi'\rangle, C', P' \rangle$  whose components are black-box extensions of the components of  $Q_1$ .

- The input in  $Q_2$  is an extension of the input in  $Q_1$  supplemented by ancillae qubits initialized to a fixed state (wlog. in state  $|0\rangle$ ), i.e.,  $|\psi'\rangle = |\psi\rangle \otimes |00 \dots 00\rangle$ .
- The projection operator in  $Q_2$  is an extension of the projection operator in  $Q_1$  to include measurement of the ancillae in a basis independent of  $Q_1$ , i.e.,  $P' = P \otimes P_a$ .
- The number of ancillae and the operator  $P_a$  are independent of  $Q_1$  and depend upon  $\delta, \epsilon$ .
- The circuit in  $Q_2$  calls  $C$  and  $C^\dagger$  and uses additional gates that depend upon  $\delta$  and  $\epsilon$ .
- $C'$  may also use gates that depend upon  $P_E$  and  $|\psi\rangle$ .

We call the transformations that satisfy the final condition as “non-uniform” since the transformed circuit could be using gates that depend upon the input states and measurement operators of the respective

<sup>1</sup>The same question for classical classes was asked here: <http://csttheory.stackexchange.com/questions/20027/in-what-class-are-randomized-algorithms-that-err-with-exactly-25-chance>.

quantum system. Note that the non-uniformity is not with respect to  $n$ , the number of qubits of the quantum system, but with respect to the gates of the transformed circuit. It will be clear from the proof of Theorem 4 that the transformations that will be used in this paper are anyway uniform in  $n$ . In any case, we will always drop  $n$  from the superscript of  $\mathcal{B}_{\delta,\epsilon}^n$ . We will revisit the notion of non-uniformity in Section 4.

We want transformed quantum circuits that solve the quantum distinguishing problem without any error which motivates the next definition.

**Definition 2.** For a set of quantum systems  $\mathcal{S} = \{\mathcal{Q}_1, \mathcal{Q}_2, \dots\}$  with output distributions either  $\mu_p$  or  $\mu_q$  (for  $p < q$ ), a  $\mathcal{B}$ -transform  $\mathcal{B}$  is said to solve  $QD(\mathcal{S})$  with error  $(\delta, \epsilon)$ , in other words  $\mathcal{B}$  is a  $(\delta, \epsilon)$ -solution of  $QD(\mathcal{S})$ , if the following holds for some  $\delta < \epsilon$  and all  $\mathcal{Q} \in \mathcal{S}$ .

- If  $\mu(\mathcal{Q}) = \mu_p$ , then outcome of  $\mathcal{B}(\mathcal{Q})$  is  $E$  with probability  $\delta$ .
- If  $\mu(\mathcal{Q}) = \mu_q$ , then outcome of  $\mathcal{B}(\mathcal{Q})$  is  $E$  with probability  $\epsilon$ .

$QD(\mathcal{S})$  is said to have a perfect solution if  $\mathcal{B}$  is a  $(0, 1)$ -solution of  $QD(\mathcal{S})$ .

It can be seen that the identity  $\mathcal{B}$ -transform is a trivial solution of the above  $QD(\mathcal{S})$  with error  $(p, q)$ . The last part of the above definition is based on the fact that if  $\mathcal{B}$  is a  $(0, 1)$ -solution of  $QD(\mathcal{S})$ , then the outcome of  $\mathcal{Q}' = \mathcal{B}(\mathcal{Q})$  can be used to correctly infer the output distribution of any given instance  $\mathcal{Q} \in \mathcal{S}$ . Let  $\mathcal{Q}' = \mathcal{B}(\mathcal{Q})$  – which is essentially an extension of the input of  $\mathcal{Q}$  with some ancillae, an extension of its measurement operator and a circuit that can call the circuits of  $\mathcal{Q}$  (and its inverse) in a black-box manner. If the output distribution of  $\mathcal{Q}$  is  $\mu_p$ , then the outcome of  $\mathcal{Q}'$  is never  $E$  and otherwise (i.e., if the output distribution of  $\mathcal{Q}$  is  $\mu_q$ ) the outcome of  $\mathcal{Q}'$  is always  $E$  without any error.

The main theorem of our work is stated next.

**Theorem 4.** Let  $\mathcal{S} = \{\mathcal{Q}_1, \mathcal{Q}_2, \dots\}$  be a collection of quantum systems such that output distribution of any  $\mathcal{Q}_i \in \mathcal{S}$  is either  $\mu_\delta$  or  $\mu_\epsilon$  for some  $\delta < \epsilon$ . Then  $\mathcal{S}$  is perfectly-solvable via some  $\mathcal{B}$ -transition  $\mathcal{B}_{\delta,\epsilon}$ , i.e., any  $\mathcal{Q}_i \in \mathcal{S}$  can be transformed by  $\mathcal{B}_{\delta,\epsilon}$  to some  $\mathcal{Q}'_i$  such that:

- if output distribution of  $\mathcal{Q}_i$  is  $\mu_\delta$ , then outcome of  $\mathcal{Q}'_i$  is never  $E$  and
- if output distribution of  $\mathcal{Q}_i$  is  $\mu_\epsilon$ , then outcome of  $\mathcal{Q}'_i$  is always  $E$ .

The proof of this theorem is presented in the next section. Note that, unlike Theorem 2 which only applies to one-sided error algorithms, we prove that two-sided error algorithms can also be “amplified to certainty”. A straight-forward application of this is to exactly distinguish between two QS with known output distributions, such as Theorem 1 (Section 1).

*Proof of Theorem 1.* Consider the transformation  $\mathcal{B}_{\delta,\epsilon}^n$  from Theorem 4. Given an  $n$ -qubit  $\mathcal{Q} = \langle |\psi\rangle, C, \mathcal{P} \rangle$ , construct the transformed QS  $\mathcal{B}_{\delta,\epsilon}^n(\mathcal{Q}) = \langle |\psi\rangle \otimes |\mathbf{00} \dots \mathbf{0}\rangle, C', \mathcal{P} \otimes \mathcal{P}_a \rangle$ . By Theorem 4, the output state of the transformed circuit  $C'$ , when given  $|\psi\rangle$  (along with a few ancillae in a fixed state), upon measurement by a simple extension of  $\mathcal{P}$ , has outcome either  $E$  or  $F$ , depending upon whether  $\mu(\mathcal{Q}) = \mu_\delta$  or  $\mu(\mathcal{Q}) = \mu_\epsilon$ .  $\square$

### 3 Proof of Theorem 4

We first state and prove our main technical tool – the *Separability Lemma* which essentially amplifies amplitudes of one-sided error algorithms. The Lemma can be proven using already known techniques of amplitude amplifications (e.g., see [7, Sec 2.1]). We give an alternative recursive construction that is optimized towards amplifying fixed probabilities.

We use the following notation for the sake of brevity. Given a collection of quantum systems  $\{\mathcal{Q}_1, \mathcal{Q}_2, \dots\}$  (such collections will be always denoted by  $\mathcal{S}$ ), we say that  $\mathcal{S}$  is  $(\delta, \epsilon)$ -separable (for some  $\delta < \epsilon$ ) if output distribution of any  $\mathcal{Q}_i$  in  $\mathcal{S}$  is either  $\mu_\delta$  or  $\mu_\epsilon$ .

**Lemma 1.** [Separability] For  $\delta < \epsilon < 1$  and a collection of quantum systems  $\mathcal{S}_1$  which is  $(\delta, \epsilon)$ -separable, there is a  $\mathcal{B}$ -transform  $\mathcal{B}_\epsilon$  which converts  $\mathcal{S}_1$  to a  $(\delta', 1)$ -separable collection of quantum systems (for some  $\delta \leq \delta' < 1$ ). Additionally,  $\delta = \delta' = 0$  if and only if  $\delta = 0$ .

Range of initial probability $p$	Optimum $\alpha = \theta$	Relative increase $\frac{p'}{p} = \Delta_p^*$	Amplified probability $p' = p\Delta_p^*$
$p = 0.5$	$\pi/2$	2	1
$0.25 \leq p \leq 0.5$	$\arccos\left(1 - \frac{1}{2p}\right)$	$\frac{1}{p}$	1
$p \leq 0.25$	$\pi$	$(3 - 4p)^2 \geq 4$	$p(3 - 4p)^2 \geq 4p$

Table 1: Optimum Grover iterator for different values of initial probability

Given an instance  $\mathcal{Q} = \langle |\psi\rangle, C, \mathcal{P} \rangle$  of some  $\mathcal{Q}_i \in \mathcal{S}_1$ , Lemma 1 gives us a way to determine whether the distribution of  $\mathcal{Q}$  is  $\langle 0, 1 \rangle$  or  $\langle \epsilon, 1 - \epsilon \rangle$  by first transforming  $\mathcal{Q}$  to  $\mathcal{B}(\mathcal{Q}) = \mathcal{Q}' = \langle |\psi'\rangle, C', \mathcal{P}' \rangle$  and then measuring the output of  $C'$  on  $|\psi'\rangle$  (which is a simple extension of the original input state) using measurement operator  $\mathcal{P}'$  (which is also a simple extension of the original measurement operator).

### 3.1 Grover iterator

As is usual in all analysis of amplitude amplification, the main operator to study is the Grover iterator [8, 7]. Suppose we have a circuit  $C$  acting on an input state  $|\psi\rangle$  and supposed to be measured using a two-output projective measurement operator  $\mathcal{P} = \langle P_E, I - P_E \rangle$ . We consider a generalized version, similar to the one studied by Høyer [9]:  $G(C, |\psi\rangle, \mathcal{P}, \theta, \alpha) = CS_{|\psi\rangle}C^\dagger S_{\mathcal{P}}C$  using these additional gates:  $S_{|\psi\rangle} = I - (1 - e^{i\theta})|\psi\rangle\langle\psi|$  and  $S_{\mathcal{P}} = I - (1 - e^{i\alpha})P_E$ .

Let  $|\psi'\rangle = C|\psi\rangle$  denote the output state,  $|\psi_E\rangle = P_E|\psi'\rangle$  and  $p$  denote  $\langle\psi_E|\psi_E\rangle$  – the probability of measuring outcome  $E$  for this output state.

It is easy to see that  $CS_{|\psi\rangle}C^\dagger = I - (1 - e^{i\theta})|\psi'\rangle\langle\psi'|$  and  $S_{\mathcal{P}}C|\psi\rangle = (I - (1 - e^{i\alpha})P_E)|\psi'\rangle$ . One can then compute  $|\psi''\rangle = G|\psi\rangle$  as  $(e^{i\theta} + (1 - e^{i\alpha})(1 - e^{i\theta})p)|\psi'\rangle - (1 - e^{i\alpha})|\psi_E\rangle$  and  $P_E|\psi''\rangle = (e^{i\theta} + e^{i\alpha} - 1 + (1 - e^{i\alpha})(1 - e^{i\theta})p)|\psi_E\rangle$ .

We get the following lemma summarizing the relative increase in probability after one application of our Grover iterator. We will use  $p'(\theta, \alpha, p)$  to denote the new probability of measuring outcome  $E$  on the output state after applying  $G$  on input  $|\psi\rangle$ .

**Lemma 2.** *Given a quantum system  $\mathcal{Q}_1 = \langle |\psi\rangle, C, \mathcal{P} \rangle$  and  $\alpha, \theta \in [0, \pi]$ , let  $G$  be the circuit for the Grover iterator  $G(C, |\psi\rangle, \mathcal{P}, \theta, \alpha) = CS_{|\psi\rangle}C^\dagger S_{\mathcal{P}}C$ . If  $p$  denotes the probability of observing outcome  $E$  for  $\mathcal{Q}_1$  and  $p'$  denotes the same probability for the QS  $\langle |\psi\rangle, G, \mathcal{P} \rangle$ , then  $p' = p\Delta$  where  $\Delta = |(e^{i\theta} + e^{i\alpha} - 1 + (1 - e^{i\alpha})(1 - e^{i\theta})p)|^2$ .*

First,  $p = 0$  if and only if  $p' = 0$  which means amplification has no effect on impossible outcomes. On the other hand, if  $p > 0$ ,  $p'$  is maximized when  $\theta = \alpha$ ; it can be shown that  $\Delta = ((1 - 2p)\cos\theta - 2(1 - p))^2 + \sin^2\theta$  in that case. We will use  $\Delta_p^*$  to denote the maximum value of  $\Delta$  for any  $p$  and using optimal  $\theta$  and  $\alpha$ . The corresponding *optimal Grover iterator* will be denoted as  $G_p^*(C, |\psi\rangle, \mathcal{P})$ ; note that  $G^*$  increases the probability from  $p$  to  $p' = p\Delta_p^*$ . Table 1 summarizes the optimum value of  $p'$  and the relative increase for different possible values of initial probability  $p$ . Details of the relevant calculations are given in Appendix.

The following definition and corollary essentially describes the optimum  $\mathcal{B}$ -transform.

**Definition 3** (Optimal  $\mathcal{B}$ -transform).  $\mathcal{B}_p^* : \langle |\psi\rangle, C, \mathcal{P} \rangle \longrightarrow \langle |\psi\rangle, G_p^*(C, |\psi\rangle, \mathcal{P}), \mathcal{P} \rangle$

**Corollary 1.** *If the output distribution of a QS  $\mathcal{Q}$  is  $\mu_\epsilon$ , then the output distribution of  $\mathcal{B}_\epsilon^*(\mathcal{Q})$  is  $\langle \epsilon\Delta_\epsilon^*, 1 - \epsilon\Delta_\epsilon^* \rangle$ . On the other hand, if the output distribution is  $\mu_\delta$  (for some  $\delta < \epsilon$ ), then the output distribution of  $\mathcal{B}_\epsilon^*(\mathcal{Q})$  is  $\langle \delta', 1 - \delta' \rangle$  for some  $\delta' \geq \delta$  which can be computed using  $\delta$  and  $\epsilon$ . Furthermore,  $\delta = \delta'$  if and only if  $\delta = 0$  (in which case,  $\delta' = 0$ ).*

In the next few subsections, we prove Separability Lemma for different values of  $\epsilon$ .

### 3.2 $\mathcal{B}_\epsilon$ for $\epsilon \in [1/4, 1/2]$

This is the simplest of all cases, to  $\mathcal{B}$ -transform  $(\delta, \epsilon)$ -separable  $\mathcal{S}_1$  to a  $(\delta', 1)$ -separable one, for any  $1/4 \leq \epsilon \leq 1/2$  and for some  $\delta \leq \delta'$ . We can clearly use  $\mathcal{B}_\epsilon = \mathcal{B}_\epsilon^*$  defined in Definition 3. Separability Lemma immediately follows from Corollary 1 and Table 1.

### 3.3 $\mathcal{B}_\epsilon$ for $\epsilon > \frac{1}{2}$

We use the idea proposed by Brassard et al. [7] to first convert  $\mathcal{S}_1$  to a  $(\delta', \frac{1}{2})$ -separable  $\mathcal{S}_2$ ; let  $\mathcal{B}_\epsilon^+$  denote this transformation which is illustrated in Equation 1. This involves an additional qubit in state  $|0\rangle$  and an additional projective operator  $\mathcal{P}_\epsilon = \langle P_\epsilon^0, I - P_\epsilon^0 \rangle$ , where,

$$P_\epsilon^0 = \frac{1}{2\epsilon}|0\rangle\langle 0| + \sqrt{1 - \frac{1}{2\epsilon}}\sqrt{\frac{1}{2\epsilon}}|1\rangle\langle 0| + \sqrt{1 - \frac{1}{2\epsilon}}\sqrt{\frac{1}{2\epsilon}}|0\rangle\langle 1| + (1 - \frac{1}{2\epsilon})|1\rangle\langle 1|$$

Then we convert  $\mathcal{S}_2$  to a  $(\delta'', 1)$ -separable  $\mathcal{S}_3$  by using  $\mathcal{B}_{\frac{1}{2}}$  (see Subsection 3.2). Combining both of these, we propose the following transformation for  $\mathcal{B}_\epsilon$ . Here  $\mathcal{P}'$  denotes  $\mathcal{P} \otimes \mathcal{P}_\epsilon$ .

$$\langle |\psi\rangle, C, \mathcal{P} \rangle \xrightarrow{\mathcal{B}_\epsilon^+} \langle |\psi\rangle \otimes |0\rangle, C \otimes I, \mathcal{P}' \rangle \xrightarrow{\mathcal{B}_{\frac{1}{2}}} \langle |\psi\rangle \otimes |0\rangle, G_{1/2}^*(C \otimes I, |\psi\rangle \otimes |0\rangle, \mathcal{P}'), \mathcal{P}' \rangle \quad (1)$$

*Proof of Separability Lemma:* The transformation from  $\mathcal{S}_2$  to  $\mathcal{S}_3$  was shown to be correct in Subsection 3.2. Correctness of  $\mathcal{B}_\epsilon^+$  follows from the fact that the probability of measuring outcome 0 on the state  $|0\rangle$  is  $\frac{1}{2\epsilon}$  (since  $\frac{1}{2} < \epsilon \leq 1$ ,  $\frac{1}{2} \leq \frac{1}{2\epsilon} < 1$ ). Let  $p$  denote the probability of measuring outcome  $E$  for some  $\mathcal{Q} = \langle |\psi\rangle, C, \mathcal{P} \rangle \in \mathcal{S}_1$  and let  $p'$  denote the same probability for the QS  $\langle |\psi\rangle \otimes |0\rangle, C \otimes I, \mathcal{P} \otimes \mathcal{P}_\epsilon \rangle$  of  $\mathcal{S}_2$ . Observe that, if  $p = 0$ , then  $p' = 0$ ; furthermore, if  $p = \epsilon > \frac{1}{2}$ , then  $p' = \epsilon \frac{1}{2\epsilon} = \frac{1}{2}$ . Of course, the transformation does not depend upon  $\delta$ .  $\square$

### 3.4 $\mathcal{B}_\epsilon$ for $\epsilon < \frac{1}{4}$

To transform  $(\delta, \epsilon)$ -separable  $\mathcal{S}_1$  to  $(\delta', 1)$ -separable one, we first repeatedly apply the optimum Grover iterator enough number of times to amplify  $\epsilon$  beyond  $\frac{1}{4}$  and then apply a suitable  $\mathcal{B}_{\epsilon_k}$  from Subsection 3.2.

Suppose  $\epsilon < 1/4$ . Let  $\epsilon_1 = \epsilon \Delta_\epsilon^*$ ,  $\epsilon_2 = \epsilon_1 \Delta_{\epsilon_1}^*$ ,  $\epsilon_3 = \epsilon_2 \Delta_{\epsilon_2}^*, \dots$ . Let  $k$  be the smallest integer such that  $\epsilon_k \geq 1/4$ ; clearly,  $\epsilon_1, \dots, \epsilon_{k-1} < 1/4$  and  $\epsilon_k \in [1/4, 1/2]$ . We define  $\mathcal{B}_\epsilon$  as the  $k$  transformations  $\mathcal{B}_\epsilon^*, \mathcal{B}_{\epsilon_1}^*, \mathcal{B}_{\epsilon_2}^*, \dots, \mathcal{B}_{\epsilon_{k-1}}^*$  applied successively and then followed by  $\mathcal{B}_{\epsilon_k}$ .

$$\begin{aligned} \mathcal{B}_\epsilon : \langle |\psi\rangle, C, \mathcal{P} \rangle &\xrightarrow{\mathcal{B}_\epsilon^*} \langle |\psi\rangle, C_1, \mathcal{P} \rangle && \text{output dist.} = \langle \epsilon_1, 1 - \epsilon_1 \rangle \ \& \ C_1 = G_\epsilon^*(C, |\psi\rangle, \mathcal{P}) \\ &\xrightarrow{\mathcal{B}_{\epsilon_1}^*} \langle |\psi\rangle, C_2, \mathcal{P} \rangle && \text{output dist.} = \langle \epsilon_2, 1 - \epsilon_2 \rangle \ \& \ C_2 = G_{\epsilon_1}^*(C_1, |\psi\rangle, \mathcal{P}) \\ &\xrightarrow{\mathcal{B}_{\epsilon_2}^*} \dots && \dots \\ &\xrightarrow{\mathcal{B}_{\epsilon_{k-1}}^*} \langle |\psi\rangle, C_k, \mathcal{P} \rangle && \text{output dist.} = \langle \epsilon_k, 1 - \epsilon_k \rangle \ \& \ C_k = G_{\epsilon_{k-1}}^*(C_{k-1}, |\psi\rangle, \mathcal{P}) \\ &\xrightarrow{\mathcal{B}_{\epsilon_k}} \langle |\psi\rangle, C_{k+1}, \mathcal{P}' \rangle \end{aligned}$$

*Proof of Separability Lemma:* Satisfiability Lemma is easily proved by observing that  $\epsilon_k \in [1/4, 1/2]$  and so, applying  $\mathcal{B}_{\epsilon_k}$  (from Subsection 3.2) at the last step ensures that the final QS has output distribution  $\langle 1, 0 \rangle$ . It is also easy to check that these output distributions remain unchanged if and only if  $\delta = 0$ .  $\square$

### 3.5 Performance Evaluation

Even though we propose a recursive approach to reduce error-probability of exact error quantum systems, we show that our approach is essentially same as the existing iterative approaches for amplitude amplification in terms of the number of calls to  $C$  and  $C^\dagger$ .

Take any quantum system  $QS = \langle |\psi\rangle, C, \mathcal{P} \rangle$ . The existing approaches [7, 9] repeatedly apply the iterative Grover operator  $\mathcal{Q} = (CS_{|\psi\rangle}C^\dagger S_{\mathcal{P}})$  (generalized to act on input encoded as the initial state and output state to be measured by any projective operator) on  $C|\psi\rangle$ . Here  $S_{|\psi\rangle}$  and  $S_{\mathcal{P}}$  modify the phase of certain states by  $\theta = \alpha = \pi$  as specified in Subsection 3.1.

Let  $\epsilon$  denote the probability of observing outcome  $E$ ; let  $\beta \in [0, \pi/2]$  be such that  $\sin^2 \beta = \epsilon$ . Then, the probability of observing  $E$  on repeated applications of  $\mathcal{Q}$ , say  $b$  times, on  $C|\psi\rangle$  (i.e., on the output state of  $\mathcal{Q}^b C|\psi\rangle$ ) can be shown to be  $\sin^2((2b+1)\beta)$ .

As shown in Table 1, suitably choice of phases in  $S_{|\psi\rangle}$  and  $S_{\mathcal{P}}$  can amplify any  $\epsilon \in [0.25, 1]$  to 1 using a  $\mathcal{B}$ -transform that effectively corresponds to one application of  $\mathcal{Q}$  on  $C|\psi\rangle$ . So, if  $\epsilon \geq 0.25$ , our recursive method and the iterative approach are identical.

So, we will now analyze  $\mathcal{B}_\epsilon$  for  $\epsilon < 0.25$ , in fact, for  $\epsilon \ll 0.25$ . Let  $k$  be the number of  $\mathcal{B}^*$ -transforms required. Recall from Subsection 3.4 that  $\mathcal{B}_\epsilon$  keeps the input and the projective operator unchanged

and converts  $C$  to some  $C_{k+1}$  via intermediate circuits  $C_1, C_2, \dots, C_k$  where  $C_{j+1} = G_{\epsilon_j}^*(C_j, |\psi\rangle, \mathcal{P})$  for  $\epsilon < \epsilon_1 < \dots < \epsilon_k \in [1/4, 1/2]$ . The  $S_{|\psi\rangle}$  and  $S_{\mathcal{P}}$  operators in those  $G^*$  are defined using phases  $\theta = \alpha = \pi$  as per Table 1.

**Lemma 3.** For any  $j \in [1, k]$ ,  $C_j = \mathcal{Q}^{\frac{3^j-1}{2}} C$ .

This lemma can be easily proved by induction on  $k$  (see Appendix). It shows that the final circuit obtained by our recursive approach is identical to that obtained by apply a fixed  $\mathcal{Q}$  a certain number of times. Therefore,  $\epsilon_k = \sin^2(3^k \beta)$  which must be at least  $1/4$ . This stipulates that  $k \geq \log_3 \frac{\pi}{6\beta}$ . The total number of calls to  $C$  and  $C^\dagger$  made by our recursive algorithm to amplify  $\epsilon < 0.25$  to some  $\epsilon_k > 0.25$  can then be easily shown to be  $1 + \frac{\pi}{3\beta}$  (rather, the next higher integer) – which is exactly the same as that in  $\mathcal{Q}^{(3^k-1)/2} C$ .

### 3.6 Proof of Theorem 4

We are now ready to prove Theorem 4 using Separability Lemma. We will use the following notation. If  $\mathcal{B}$  is a transformation for a set of quantum systems  $\mathcal{S}$ , then the set of *transformed quantum systems* after applying  $\mathcal{B}$  will be denoted by  $\mathcal{B}(\mathcal{S})$ .

*Proof.* The given  $\mathcal{S}$  in the theorem is  $(\delta, \epsilon)$ -separable. Our required  $\mathcal{B}_{\delta, \epsilon}$  will be composed of a series of  $\mathcal{B}$ -transforms:  $\mathcal{B}_\epsilon$ ,  $\mathcal{B}_2$  and  $\mathcal{B}_\delta$ .

$\mathcal{B}_\epsilon$  is chosen such so as to solve  $QD(\mathcal{S})$  with error  $(\delta', 1)$  for some  $\delta < \delta'$ . This step can be skipped ( $\mathcal{B}_\epsilon$  can be set to identity) if  $\epsilon = 1$ ; on the other hand, if  $\epsilon < 1$ , we can use  $\mathcal{B}_\epsilon$  from Lemma 1, which implies that  $\mathcal{B}_\epsilon(\mathcal{S})$  is  $(\delta', 1)$ -separable for some  $\delta'$  (that depends on  $\delta$  and  $\epsilon$ ). Let  $\mathcal{S}_1$  denote  $\mathcal{B}_\epsilon(\mathcal{S})$ .

$\mathcal{B}_2$  is the following transform:  $\langle |\psi\rangle, C, (P_1, P_2) \rangle \rightarrow \langle |\psi\rangle, C, (P_2, P_1) \rangle$ . Let  $\mathcal{S}_2 = \mathcal{B}_2(\mathcal{S}_1)$ . Any  $QS \in \mathcal{S}_1$  with  $\mu(QS) = \mu_{\delta'}$  is transformed to  $QS' \in \mathcal{S}_2$  with  $\mu(QS') = 1 - \delta'$  and similarly, if  $\mu(QS) = \mu_1$ , then  $\mu(QS') = \mu_0$ . Therefore,  $\mathcal{S}_2$  is  $(0, 1 - \delta')$ -separable.

By property of  $\mathcal{B}_\epsilon$ ,  $\delta = \delta' = 0$  if and only if  $\delta = 0$  and in that case, we have obtained  $(0, 1)$ -separable  $\mathcal{S}_2$ . On the other hand, if  $\delta > 0$ , then  $\delta' > 0$ . Let  $\delta''$  denote  $1 - \delta'$ . Since  $\mathcal{S}_2$  is  $(0, \delta'')$ -separable, apply Lemma 1 again to get  $\mathcal{B}_\delta$  such that  $\mathcal{S}' = \mathcal{B}_\delta(\mathcal{S}_2)$  is  $(0, 1)$ -separable.

Our required transform  $\mathcal{B}$  is a sequential application of  $\mathcal{B}_\epsilon$  followed by  $\mathcal{B}_2$  followed by  $\mathcal{B}_\delta$ . As explained above,  $\mathcal{B}_\delta(\mathcal{B}_2(\mathcal{B}_\epsilon(\cdot)))$  is a  $(0, 1)$ -solution of  $QD(\mathcal{S})$ .  $\square$

## 4 Uniform version of Theorem 4

The non-uniformity in Definition 1 is not very helpful if we wish to obtain a true black-box extension of a quantum system  $\mathcal{Q} = \langle |\psi\rangle, C, \mathcal{P} \rangle$ . Note that the extension to the input qubits and the extension to the projective measurement operator is anyway independent of  $\mathcal{Q}$  and  $n$ , the gates in  $C'$  are uniform in  $n$ , and furthermore, the transformed circuit  $C'$  is allowed to call the original circuit  $C$  (and its inverse  $C^\dagger$ ) in a black-box manner; however, some of the gates in  $C'$  may additionally depend upon  $|\psi\rangle$  and operators of  $\mathcal{P}$ . It would be really good to obtain a more uniform conversion which necessitates the following definition.

**Definition 4** (Uniform  $\mathcal{B}$ -transform). A  $\mathcal{B}$ -transform for converting multiple  $QS \{ \mathcal{Q}_1, \mathcal{Q}_2, \dots \}$  is said to be uniform if the circuit of  $\mathcal{B}(\mathcal{Q}_i)$  is identical for all source  $\mathcal{Q}_i$  except for the calls to  $C$  and  $C^\dagger$  corresponding to  $\mathcal{Q}_i$ .

### 4.1 Uniform Grover iterator

We want to study some sufficient conditions for the  $\mathcal{B}$ -transforms to be uniform by constructing a uniform version of Grover iterator.

Since Grover iterator uses  $\mathcal{S}_{\mathcal{P}}$ , it is crucial to have identical measurement operators for all quantum systems. This is, however, not such a major requirement since it is always possible to change measurement operators by extending a quantum circuit with suitable operators.

Except the gates  $S_{|\psi\rangle} = I - (1 - e^{i\theta})|\psi\rangle\langle\psi|$  which depend upon the corresponding input to the circuit ( $|\psi\rangle$ ), none of the other gates used in  $\mathcal{B}$ -transforms that are involved in the proof of Theorem 4 depend

upon the input state (see Section 3). However, a  $\mathcal{B}$ -transform may still become uniform if all the inputs in  $\mathcal{S}_1$ , and hence all such  $S_{|\psi\rangle}$  gates, will be identical.

Now consider a second option – all measurement operators are identical and all the input states are not identical but they form an orthonormal set. We show that it is still possible to apply  $S_{|\psi\rangle}$  in a uniform manner. Recall that this gate changes the phase of any state depending upon whether it is  $|\psi\rangle$  or not and the main difficulty appears to be the fact that the input state cannot be copied and stored for a later application of the conditional phase gate. So our main idea is to convert  $|\psi\rangle$  to some state in the standard basis since it is possible to copy and store states in the standard basis using the *quantum fanout gate* [4]. This gate copies a standard basis state to another register:  $F_m|x_1 \dots x_m\rangle|b_1 \dots b_m\rangle = |x_1 \dots x_m\rangle|(x_1 \oplus b_1) \dots (x_m \oplus b_m)\rangle$  for  $x_1 \dots x_m \in \{0, 1\}^m$  and  $b_1 \dots b_m \in \{0, 1\}^m$  shows the operation for “copying”  $m$ -qubits.

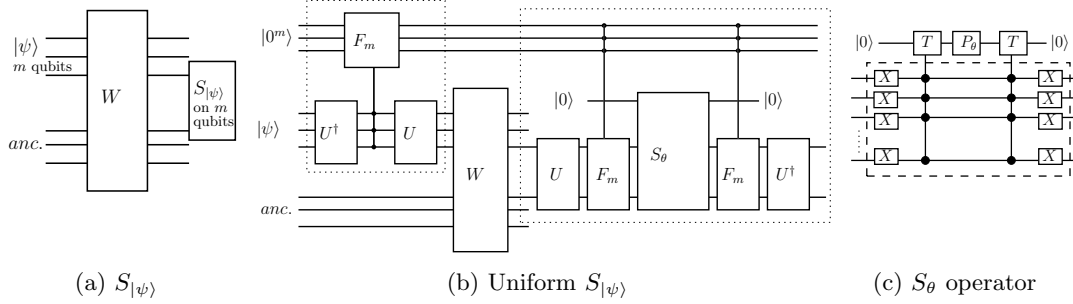


Figure 2: Applying operator  $S_{|\psi\rangle}$  in a uniform manner. Figure 2a shows the non-uniform operator and Figure 2b shows its uniform version (dotted box on the left shows initialization and dotted box on the right shows  $S_{|\psi\rangle}$  being applied uniformly). Figure 2c shows the  $S_\theta$  operator from Figure 2b.

See Figure 2 for a uniform version of  $S_{|\psi\rangle}$ . Figure 2a shows  $S_{|\psi\rangle}$  as a part of an arbitrary quantum circuit, say  $C$  that takes as input an  $m$ -qubit state  $|\psi\rangle$  (and some ancillæ) and  $S_{|\psi\rangle}$ , on  $m$ -qubits, is one of its gates. Since we are now considering the case that  $C$  is applied only on orthogonal input states (suppose denoted by  $|\psi_1\rangle, |\psi_2\rangle, \dots$ ), therefore, there exists a one to one mapping between these states and a subset of the  $m$ -qubit standard basis states  $|1\rangle, |2\rangle, \dots$ . Let  $U$  denote the unitary operator for the mapping, i.e.,  $U|\psi_v\rangle = |v\rangle$ .

Figure 2b illustrates a circuit  $C'$  that applies  $S_{|\psi\rangle}$  without requiring a gate that explicitly depends upon  $|\psi\rangle$ . Apart from the two registers of  $C$  (the input  $|\psi\rangle$  and ancillæ qubits),  $C'$  also uses  $m$  additional ancillæ qubits in state  $|0\rangle$ . Other than the standard gates ( $T$  stands for the unbounded fanout Toffoli and  $X$  is the quantum NOT gate),  $C'$  uses three additional gates:  $F_m$ ,  $P_\theta$  and  $S_\theta$ . The  $F_m$  gate is the quantum fanout gate.  $P_\theta$  changes phase of  $|1\rangle$  by  $e^{i\theta}$ :  $P_\theta = I - (1 - e^{i\theta})|0\rangle\langle 0|$ . The  $S_\theta$  gate uses an additional reusable ancillæ  $|0\rangle$  and changes the phase by  $e^{i\theta}$  only for the state  $|0^m\rangle$  (illustrated in Figure 2c).

The state of the first two registers after the left dotted box in Figure 2b is simply  $|0^m\rangle|\psi\rangle \rightarrow |v\rangle|\psi\rangle$  where  $|v\rangle$  is the standard basis vector  $U|\psi\rangle$ . We will next analyze the operator for the right dotted box, say denoted by  $U_R$ .  $S_\theta$  can be written as  $I - (1 - e^{i\theta})|0^m\rangle\langle 0^m|$  and the  $F_m$  operator essentially behaves like  $F_m|b_1 \dots b_m\rangle \rightarrow |(v_1 \oplus b_1), \dots (v_m \oplus b_m)\rangle$ . The following calculation (for only the qubits involved) shows that the operator for the right dotted box is identical with  $S_{|\psi\rangle}$ .

$$\begin{aligned} U_R &= (I \otimes U^\dagger) F_m (I \otimes S_\theta) F_m (I \otimes U) = (I \otimes U^\dagger) F_m (I \otimes (I - (1 - e^{i\theta})|0^m\rangle\langle 0^m|)) F_m (I \otimes U) \\ &= (I \otimes U^\dagger) (I \otimes (I - (1 - e^{i\theta})|v\rangle\langle v|)) (I \otimes U) = I \otimes (I - (1 - e^{i\theta})|\psi\rangle\langle\psi|) = I \otimes S_{|\psi\rangle} \end{aligned}$$

The results of this subsection can be summarized in the following lemma.

**Lemma 4.** *The  $\mathcal{B}$ -transform in Theorem 4 can be made uniform if all projection operators in the quantum systems of  $\mathcal{S}$  are identical and all input states in  $\mathcal{S}$  are either identical or form an orthonormal set of states.*



## 5 Distinguishing two circuits

Suppose we are given a quantum circuit  $C$  (as black-box) and two different operators  $C_1$  and  $C_2$ , all acting on the same Hilbert space, and we are told that the operator for  $C$  is either  $C_1$  or  $C_2$ . We have to determine  $C$  corresponds to which one. We assume that we also have access to its inverse operator  $C^\dagger$ .

The analogous problem for deterministic (classical) functions is trivial. Two distinct functions must differ at some input which can be determined from their function descriptions (the problem is NP-hard but we are not concerned about feasibility, not efficiency, for this discussion). The output of  $C$  on this input will identify whether  $C$  is  $C_1$  or  $C_2$ . However, if  $C$  is a randomized circuit or algorithm, then except for a few trivial cases, the output of  $C$  generates a sample distribution over the output of  $C_1$  and  $C_2$ ; the question of determining the correct distribution of  $C$  without any error is believed to be hard, if not impossible.

However, it is possible to give a positive answer to the same question for quantum circuits. Select a suitable  $|\phi\rangle$  and compute the two possible output states  $|\psi_1\rangle = C_1|\phi\rangle$ ,  $|\psi_2\rangle = C_2|\phi\rangle$ . Choose projective operators  $\mathcal{P} = \langle I - |\psi_1\rangle\langle\psi_1|, |\psi_1\rangle\langle\psi_1| \rangle$  with respective outcomes  $E$  and  $F$ .

Consider these two quantum systems:  $\langle |\phi\rangle, C_1, \mathcal{P} \rangle$  and  $\langle |\phi\rangle, C_2, \mathcal{P} \rangle$ . The output distribution of the first QS is  $\langle 0, 1 \rangle$  and that of the second is  $\langle \epsilon, 1 - \epsilon \rangle$  where  $\epsilon = 1 - |\langle \psi_1 | \psi_2 \rangle|^2 > 0$ .

Now, Theorem 4 can be applied on the QS  $\langle |\phi\rangle, C, \mathcal{P} \rangle$  which essentially gives us a circuit  $C'$  (that calls  $C$  and  $C^\dagger$ ) along with suitably extended input and measurement operators, with the property that if the outcome of the QS is  $E$ , then  $C$  is surely  $C_1$  and otherwise  $C_2$ .

It is perfectly okay to use any  $|\phi\rangle$  as the input state; however, since the size of  $C'$  depends inversely upon  $\epsilon$  so it makes sense to have the largest possible  $\epsilon$ . A recent result [2] can be used to determine the optimum initial state (details of this is presented in the Appendix).

**Single-fault detection** Fault detection is a major step in the workflow of circuit fabrication. It is common in research and industry to assume that practically most faults appear according to a few known fault models. A standard approach to detecting if a circuit is faulty is to generate a set of test patterns (inputs) such that the output of a fault-free circuit would be different from that of a faulty-circuit. This method is known as ATPG (automatic test-pattern generation) and is well-studied for classical circuits and very recently, seeing use even for quantum circuits [11].

ATPG is computationally difficult being NP-hard [10], and even harder for quantum circuits because the measurement output of these circuits is probabilistic, and hence even a single test pattern will generate a distribution over possible outcomes.

However, the technique described earlier in this section can come to our rescue in the special case of only one fault model, i.e., given a circuit  $C$  as a black-box unit, we wish to determine if  $C$  is fault-free (i.e.,  $C = C_1$ ) or  $C$  is faulty (with fault model  $C_2$ ). We can reliably answer this question without any chance of error using the approach described above.

## 6 Exact Error Algorithms

Usual probabilistic classes like **RP** and **BPP** are defined in terms of errors that are upper bounded by constants. They are rarely defined in terms of exact error, primarily due to the lack of robustness in definition that accompanies this concept. There is no known technique to show that the class of problems with one-sided error exactly same as 0.3 remains unchanged if the error is instead 0.301. Consider, for example, the simplified class **ERP** ( $\mathbf{P} \subseteq \mathbf{ERP} \subseteq \mathbf{RP}$ ) whose problems have randomized algorithms similar to those for **RP**, but with an additional requirement that the error is same for all “no” instances (of any length). We similarly define **EBPP** as the class of problems with exact two-sided error polynomial-time algorithms. Based on what we know,  $\mathbf{P} \neq \mathbf{ERP} \neq \mathbf{EBPP}$ . However, we were able to prove that the quantum analogs of these classes have identical complexity using our generalization of quantum amplitude amplification.

**Definition 5.**  $\mathbf{EBQP}_{\delta, \epsilon}$  is the class of languages  $L$  for which there exists a uniform family of polynomial-size quantum circuits  $\{C_n\}$ , a uniform family of states for  $a_n$  ancilla qubits  $|A_n\rangle$  and a uniform family of two-outcome projective measurement operators  $\{\mathcal{P}_n\}$  such that  $C_n$  and  $\mathcal{P}_n$  act on a space of  $n + a_n$  qubits and the following hold for any  $x \in \{0, 1\}^n$ ,  $\forall n$ :

- if  $x \notin L$ , then the output distribution of  $\langle |x\rangle \otimes |A_n\rangle, C_n, \mathcal{P}_n \rangle$  is  $\mu_\delta$  (i.e., when the output state of  $C_n$  on input state  $|x\rangle \otimes |A_n\rangle$  is measured using  $\mathcal{P}_n$ , outcome  $E$  is observed with probability  $\delta$ ) and
- if  $x \in L$ , then the output distribution of  $\langle |x\rangle \otimes |A_n\rangle, C_n, \mathcal{P}_n \rangle$  is  $\mu_\epsilon$  (i.e., outcome  $E$  is observed with probability  $\epsilon$  upon similar measurement as the above case).

$\mathbf{ERQP}_\epsilon$  is simply  $\mathbf{EBQP}_{0,\epsilon}$ . Define  $\mathbf{EBQP} = \bigcup_{\epsilon > \delta \geq 0} \mathbf{EBQP}_{\delta,\epsilon}$  and  $\mathbf{ERQP} = \bigcup_{\epsilon > 0} \mathbf{ERQP}_\epsilon$ .

Note that, unlike the usual definitions of probabilistic classes, for these classes it is not even clear if the different classes  $\mathbf{EBQP}_{\delta,\epsilon}$  for different  $\delta$  and  $\epsilon$  are identical. However, the following lemma is obvious from these definitions.

**Lemma 5.**  $\mathbf{EQP} = \mathbf{EBQP}_{0,1} = \mathbf{ERQP}_1$  and  $\mathbf{EQP} \subseteq \mathbf{ERQP} \subseteq \mathbf{EBQP}$ .

The main result of this section is a simple application of Theorem 4 and Lemma 4.

**Theorem 5.**  $\mathbf{EQP} = \mathbf{ERQP} = \mathbf{EBQP}$ .

*Proof.* We essentially need to show that  $\mathbf{EBQP} \subseteq \mathbf{EQP}$ . To prove this we will show that for any  $L$ , if  $L \in \mathbf{EBQP}_{\delta,\epsilon}$  (for any  $\epsilon > \delta \geq 0$ ), then  $L \in \mathbf{EBQP}_{0,1}$ .

Fix an arbitrary  $n$ . For any binary string  $x$  of length  $n$ , define the quantum system  $\mathcal{Q}_x = \langle |x\rangle \otimes |A_n\rangle, C_n, \mathcal{P}_n \rangle$  where  $|A_n\rangle$ ,  $C_n$  and  $\mathcal{P}_n$  are obtained from the definition of  $\mathbf{EBQP}_{\delta,\epsilon}$  and the fact that  $L \in \mathbf{EBQP}_{\delta,\epsilon}$ . Now consider these sets of quantum systems  $\mathcal{S}_n = \{\mathcal{Q}_x : x \in \{0,1\}^n\}$  for all  $n > 0$ . Clearly, there are two possible output distributions of any  $\mathcal{S}_n$ , namely,  $\mu_\delta$  and  $\mu_\epsilon$ . Since the input states in  $\mathcal{S}_n$  are orthonormal and the projection operators therein are identical, we can therefore apply Theorem 4 and Lemma 4 to obtain a uniform transformation  $\mathcal{B}_{\delta,\epsilon}$  which perfectly solves the problem of  $QD(\mathcal{S}_n)$ . Let  $\mathcal{B}_{\delta,\epsilon}(\mathcal{Q}_x) = \mathcal{Q}'_x = \langle |x\rangle \otimes |A_n\rangle \otimes |00\dots 0\rangle, C'_n, \mathcal{P}'_n \rangle$  which gives us (i) a circuit  $C'_n$  which calls  $C_n$  (and  $C_n^\dagger$ ) (ii) a two-outcome projective measurement operator  $\mathcal{P}'_n$  and a (iii) set of ancillae qubits in state  $|00\dots 0\rangle$  such that the following holds for the outcome of  $C'_n$  on  $|x\rangle \otimes |A_n\rangle \otimes |00\dots 0\rangle$  when measured using  $\mathcal{P}'_n$ .

- If  $x \notin L$ , then the output distribution of  $\mathcal{Q}'_x$  is  $\mu_0$ , i.e., the outcome is never  $E$ .
- If  $x \in L$ , then the output distribution of  $\mathcal{Q}'_x$  is  $\mu_1$ , i.e., the outcome is always  $E$ .

Therefore, we get a uniform family of circuits  $\{C'_n\}$ , a uniform family of ancillae qubits  $|A_n\rangle \otimes |00\dots 0\rangle$  and a uniform family of two-outcome projective measurement operator  $\{\mathcal{P}'_n\}$  such that the outcome of  $C'_{|x|}$  on any  $|x\rangle$ , with additional ancillae qubits in a uniformly generated state, when measured by  $\mathcal{P}'_{|x|}$  indicates whether  $x \in L$  without any probability of error. Since  $C'_n$  uses constantly many calls to  $C_n$  and  $C_n^\dagger$  along with other gates (the constant depends only on  $\delta$  and  $\epsilon$ ), this shows that  $L \in \mathbf{EBQP}_{0,1}$ .  $\square$

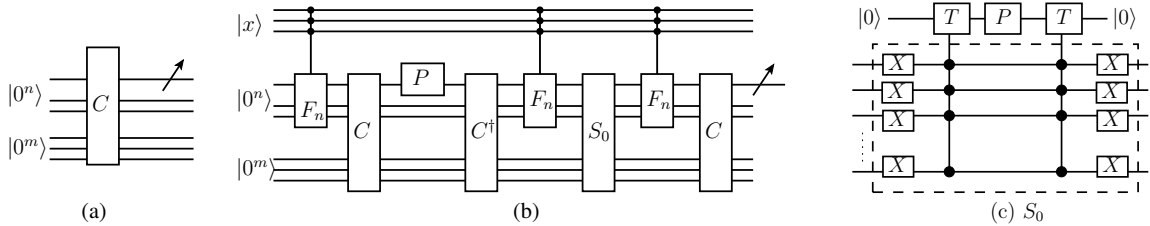


Figure 3: Circuit for  $C'$  (left) and  $S_0$  gate in  $C'$  (right)

We illustrate an application of the above theorem to obtain an error-free circuit for an  $\mathbf{ERQP}_{1/2}$  language  $L$  (see Appendix for an explicit proof). Consider circuit  $C$  in Figure 3(a) which can identify if  $x \in L$  with one-sided error 0.5. As is typical in quantum circuits, in this example only one of the output qubits of the circuit is measured in the standard basis ( $P_E = |0\rangle\langle 0| \otimes I$  and  $\mathcal{P} = \langle P_E, 1 - P_E \rangle$ ); therefore, if  $x \notin L$ , then the output qubit is never observed in state  $|0\rangle$  and if  $x \in L$ , then the output qubit is observed in states  $|0\rangle$  or  $|1\rangle$  with equal probability. The circuit  $C'$  shown in Figure 3(b) shows how to remove the probability of error; the same output qubit is measured in the standard basis for outcome and some additional qubits in state  $|0\rangle$  are used as ancillae. Apart from calling  $C$  and  $C^\dagger$ ,  $C'$  uses the

$n$ -qubit Fanout gate  $F_n$ , a conditional phase gate  $S_0$ <sup>2</sup> which changes phase of  $|00\dots 0\rangle$  by  $\iota$ , and  $P$  does the same to  $|1\rangle$ .

### 6.1 Exact amplitude amplification (Theorem 3)

*Proof of Theorem 3.* Let  $\mathcal{P}$  denote the two-outcome projective measurement operator used in the original two-sided exact error circuit  $C$ .  $C$  can be of two types depending on how it accesses its input. Any input  $x \in X$  can be accessed either through the input state  $|x\rangle$  (along with ancillæ initialized to  $|00\dots 0\rangle$ , wlog.) or through an oracle gate  $U_x : |x, b\rangle \rightarrow |x, b \oplus \Phi(x)\rangle$  (for  $b \in \{0, 1\}$ ). If  $C$  is of the former type, then Theorem 3 is essentially same as Theorem 5.

Next we focus on circuits with oracle gates. Let  $C^{U_x}$  denote this circuit when given  $U_x$  as the oracle gate corresponding to an input  $x \in X$ . The input state to  $C^{U_x}$  can be taken to be  $|00\dots 0\rangle$ , wlog. The proof follows by applying Theorem 4 on this collection of quantum systems:  $\{\langle |00\dots 0\rangle, C^{U_x}, \mathcal{P} \rangle : x \in X\}$ .

Observe that this collection satisfies the conditions of Lemma 4. So, the corresponding  $\mathcal{B}$ -transform is uniform which implies that all the transformed circuits for these quantum systems are identical, except for the calls to  $C$  and  $C^\dagger$ . Therefore, we can choose this transformed oracle circuit as our required  $C'$  of Theorem 3.  $\square$

## 7 Conclusion

Is there a classical method that can accurately decide the distribution of a random variable  $X$  among two given distributions based on multiple samples of  $X$ ? Probably no. On the other hand, if the random variables come from a quantum source, we show that quantum circuits exist that can do the same without any probability of error. A quantum circuit, along with an input state and a measurement operator, can be consider as a quantum source of samples drawn over the distribution of the measurement outcomes.

The underlying technique is a generalization of quantum amplitude amplification to two-sided error and for circuits without oracle gates. We used our amplification technique to distinguish between two circuits, when used as a black box, which has application in fault detection of quantum circuits. We also defined a restricted version of quantum one-sided and two-sided bounded error classes and used generalized amplification to show that those complexity classes collapse to (error-free) quantum polynomial time complexity class.

It would be interesting to investigate if this approach can be used for ATPG with more than one fault models and for amplifying standard bounded-error classes **BQP** and **RQP**.

---

<sup>2</sup> $S_0|00\dots 0\rangle = \iota|00\dots 0\rangle$  and for other states  $S_0|x_1x_2\dots x_k\rangle = |x_1\dots x_k\rangle$  (illustrated in Figure 3(c)).

## References

- [1] Esma Aïmeur, Gilles Brassard, and Sébastien Gambs. Quantum clustering algorithms. In *Proceedings of the 24th International Conference on Machine Learning, ICML '07*, pages 1–8, New York, NY, USA, 2007. ACM. URL: <http://doi.acm.org/10.1145/1273496.1273497>, doi:10.1145/1273496.1273497.
- [2] D. Bera, S. Maitra, S. Roychowdhury, and S. Chakraborty. Diagnosis of single faults in quantum circuits. *ArXiv e-prints*, December 2015. arXiv:1512.05051.
- [3] Debajyoti Bera. A different Deutsch–Jozsa. *Quantum Information Processing*, 14(6):1777–1785, 2015. URL: <http://dx.doi.org/10.1007/s11128-015-0976-2>, doi:10.1007/s11128-015-0976-2.
- [4] Christoph Durr. Quantum circuits: Fanout, parity, and counting. *arXiv preprint quant-ph/9903046*, 1999. arXiv:9903046.
- [5] Christoph Dürr, Mark Heiligman, Peter Høyer, and Mehdi Mhalla. *Automata, Languages and Programming: 31st International Colloquium, ICALP 2004, Turku, Finland, July 12–16, 2004. Proceedings*, chapter Quantum Query Complexity of Some Graph Problems, pages 481–493. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004. URL: [http://dx.doi.org/10.1007/978-3-540-27836-8\\_42](http://dx.doi.org/10.1007/978-3-540-27836-8_42), doi:10.1007/978-3-540-27836-8\_42.
- [6] Christoph Durr and Peter Høyer. A quantum algorithm for finding the minimum. *arXiv preprint quant-ph/9607014*, 1996.
- [7] M. Mosca G. Brassard, P. Høyer and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*. American Mathematical Society, 2002.
- [8] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, New York, New York, USA, July 1996. ACM Press. URL: <http://dl.acm.org/citation.cfm?id=237814.237866>, doi:10.1145/237814.237866.
- [9] Peter Høyer. Arbitrary phases in quantum amplitude amplification. *Physical Review A*, 62(5):052304, October 2000. URL: <http://link.aps.org/doi/10.1103/PhysRevA.62.052304>, doi:10.1103/PhysRevA.62.052304.
- [10] O.H. Ibarra and S.K. Sahni. Polynomially complete fault detection problems. *IEEE Transactions on Computers*, 24(3):242–249, 1975. doi:<http://doi.ieeecomputersociety.org/10.1109/T-C.1975.224205>.
- [11] Alexandru Paler, Armin Alaghi, Ilia Polian, and John P Hayes. Tomographic testing and validation of probabilistic circuits. In *Test Symposium (ETS), 2011 16th IEEE European*, pages 63–68. IEEE, 2011.

## A Proof of $\mathbf{ERQP}_{1/2} \subseteq \mathbf{EQP}$

**Lemma 6.** *If a language  $L \in \mathbf{ERQP}_{1/2}$ , then  $L \in \mathbf{EQP}$ .*

*Proof.* We will assume that the algorithms end with a measurement of a specified qubit in the computational basis – this is equivalent most other ways measurement strategies that are commonly applied.

Take any  $L \in \mathbf{ERQP}_{1/2}$ , and consider the corresponding circuit  $C$  (illustrated in Figure 3(a)). Suppose  $m$  denotes the number of ancilla qubits used by  $C$ , and  $n$  denotes the length of any input  $x$ , then  $C$  acts on  $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes m}$  and its output is given by  $|\psi\rangle = C|x\rangle|0^m\rangle$ . Without loss of generality, suppose that the first qubit is specified for measurement, then the projective measurement operator applied is  $|0\rangle\langle 0| \otimes I$ .

We will now construct an **EQP** circuit  $C'$  to decide the same language  $L$ . But first note that,  $|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$  and that, if  $x \notin L$ ,  $\langle\psi_1|\psi_1\rangle = 0$ , and if  $x \in L$ ,  $\langle\psi_1|\psi_1\rangle = 1/2 (= \langle\psi_0|\psi_0\rangle)$ . The circuit is constructed as  $C' = \mathcal{A}S_0\mathcal{A}^{-1}P\mathcal{A}$  and described in Figure 3(b).  $C'$  acts on  $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes m}$ , and we will denote the space as 3 registers  $P, Q, R$ , respectively, of  $n, n, m$  qubits. The gates will be labelled with the registers (as superscripts) they are applied on in the following description.

Besides the circuit  $C$ , which will be used always on registers  $QR$ , we will make frequent use of the *fanout* operator[4]. This, and the other components of  $C'$ , are listed below.

- The fanout operator effectively copies basis states from a control qubit to a target qubit. On two registers of  $n$  qubits each, it works as  $F_n|a_1 \dots a_n\rangle|b_1 \dots b_n\rangle = |a_1 \dots a_n\rangle|(b_1 \oplus a_1) \dots (b_n \oplus a_n)\rangle$ . Note that,  $F_n^\dagger = F_n$ .
- $\mathcal{A} = (F_n^{PQ} \otimes I) \otimes (I \otimes C^{QR})$
- $P^Q = I - (1 - i)|0\rangle\langle 0|$  is the phase gate  $P$  applied on the first qubit of register  $Q$ . Notice that, the first qubit of register  $Q$  is the measurement qubit with respect to  $C$ .
- $S_0^{QR} = I - (1 - i)|0^{n+m}\rangle\langle 0^{n+m}|$  which changes the phase of the basis state in which all qubits are in the state  $|0\rangle$ . Implementation of  $S_0$  is shown in Figure 3(c) – it requires one additional qubit initialized to  $|0\rangle$ . However this qubit is in state  $|0\rangle$  after application of this operator, so this qubit could be reused if required. This extra qubit has been left out in the description of  $C'$ .
- The input to  $C'$  will be  $|x\rangle|0^{\otimes n}\rangle|0^{\otimes m}\rangle$ .
- We will measure the first qubit of register  $Q$  in the standard basis at the end.

Next, we will describe the operation of  $C'$ .

$$\begin{aligned}
 C'|x\rangle|0^n\rangle|0^m\rangle &= C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot P^Q \cdot C^{QR} \cdot F_n^{PQ} \cdot |x\rangle|0^n\rangle|0^m\rangle \\
 &= C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot P^Q \cdot C^{QR} \cdot |x\rangle|x\rangle|0^n\rangle \\
 &= C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot P^Q \cdot |x\rangle \left( |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle \right) \\
 &= C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot |x\rangle \left( |0\rangle|\psi_0\rangle + i|1\rangle|\psi_1\rangle \right) \quad (*)
 \end{aligned}$$

We will now simplify the remaining operator.

$$\begin{aligned}
& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
&= C^{QR} \cdot F_n^{PQ} \cdot \left( I - (1 - \iota) I^P \otimes |0^{n+m}\rangle\langle 0^{n+m}| \right) \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
&= C^{QR} \cdot F_n^{PQ} \cdot \left( I - (1 - \iota) \sum_{n\text{-bit } p} |p, 0^{n+m}\rangle\langle p, 0^{n+m}| \right) \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
&= C^{QR} \cdot \left( I - (1 - \iota) \sum_{n\text{-bit } p} F_n^{PQ} |p, 0^{n+m}\rangle\langle p, 0^{n+m}| F_n^{PQ} \right) \cdot C^{\dagger QR} \\
&= C^{QR} \cdot \left( I - (1 - \iota) \sum_{n\text{-bit } p} |p, p, 0^m\rangle\langle p, p, 0^m| \right) \cdot C^{\dagger QR} \\
&= I - (1 - \iota) \sum_{n\text{-bit } p} |p\rangle\langle p| \otimes (C^{QR} |p, 0^m\rangle\langle p, 0^m| C^{\dagger QR})
\end{aligned}$$

Substituting this simplification in (\*) above,

$$\begin{aligned}
& \mathcal{C}' |x\rangle |0^n\rangle |0^m\rangle \\
&= \left( I - (1 - \iota) \sum_{n\text{-bit } p} |p\rangle\langle p| \otimes (C^{QR} |p, 0^m\rangle\langle p, 0^m| C^{\dagger QR}) \right) |x\rangle \left( |0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle \right) \\
&= |x\rangle \left( |0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle \right) - \\
&\quad (1 - \iota) \sum_{n\text{-bit } p} |p\rangle\langle p|x\rangle \otimes \left( C^{QR} |p, 0^m\rangle\langle p, 0^m| C^{\dagger QR} \right) \left( |0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle \right) \\
&= |x\rangle \left( |0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle \right) - (1 - \iota) |x\rangle \otimes \left( C^{QR} |x, 0^m\rangle\langle x, 0^m| C^{\dagger QR} \right) \left( |0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle \right) \\
&= |x\rangle \left( (|0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle) - (1 - \iota) (|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle) (\langle 0|\langle\psi_0| + \langle 1|\langle\psi_1|) (|0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle) \right) \\
&= |x\rangle \left( (|0\rangle|\psi_0\rangle + \iota |1\rangle|\psi_1\rangle) - (1 - \iota) (|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle) (\langle\psi_0|\psi_0\rangle + \iota \langle\psi_1|\psi_1\rangle) \right) \\
&= |x\rangle \left( (1 - (1 - \iota)K) |0\rangle|\psi_0\rangle + (\iota - (1 - \iota)K) |1\rangle|\psi_1\rangle \right) \text{ where, } K = \langle\psi_0|\psi_0\rangle + \iota \langle\psi_1|\psi_1\rangle \\
&= \begin{cases} \iota |x\rangle |0\rangle |\psi_0\rangle & \text{if, } x \notin L \text{ i.e., } \langle\psi_1|\psi_1\rangle = 0, \langle\psi_0|\psi_0\rangle = 1 \\ (\iota - 1) |x\rangle |1\rangle |\psi_1\rangle & \text{if, } x \in L \text{ i.e., } \langle\psi_1|\psi_1\rangle = \langle\psi_0|\psi_0\rangle = 1/2 \end{cases}
\end{aligned}$$

Measuring the first qubit of register  $Q$  therefore shows  $|1\rangle$  if and only if  $x \in L$ . □

## B Optimal values for Grover iterator

Let  $c$  denote  $(e^{i\theta} + e^{i\alpha} - 1 + (1 - e^{i\alpha})(1 - e^{i\theta})p)$ . Then,  $c^* = -(1 - p) + 2(1 - p)e^{-i\theta} + pe^{-2i\theta}$ . Therefore, if  $p > 0$ , then  $\Delta = cc^*$  which we will compute below.

Computing  $\Delta$ .

$$\begin{aligned}
\Delta &= cc^* \\
&= (1-p)^2 - 2(1-p)^2 e^{-i\theta} - p(1-p)e^{-2i\theta} \\
&\quad - 2(1-p)^2 e^{i\theta} + 4(1-p)^2 + 2p(1-p)e^{-i\theta} \\
&\quad - p(1-p)e^{2i\theta} + 2p(1-p)e^{i\theta} + p^2 \\
&= [(1-p)^2 + 4(1-p)^2 + p^2] + (e^{-i\theta} + e^{i\theta})[2p(1-p) - 2(1-p)^2] - (e^{-2i\theta} + e^{2i\theta})p(1-p) \\
&= 6p^2 - 10p + 5 + 4(1-p)(2p-1)\cos\theta - 2p\cos 2\theta + 2p^2\cos 2\theta \\
&= (-10 - 2\cos 2\theta)p + (6 + 2\cos 2\theta)p^2 + (\sin^2\theta + \cos^2\theta) + 4 + 4(1-p)(2p-1)\cos\theta \\
&= (-8 - 4\cos^2\theta)p + (4 + 4\cos^2\theta)p^2 + \sin^2\theta + \cos^2\theta + 4 + 4(1-p)(2p-1)\cos\theta \\
&= \sin^2\theta + (4p^2 - 4p + 1)\cos^2\theta + 4 + 4p^2 - 8p + 4(1-p)(2p-1)\cos\theta \\
&= \sin^2\theta + (2p-1)^2\cos^2\theta + 4(1-p)^2 + 4(1-p)(2p-1)\cos\theta \\
&= [(2p-1)\cos\theta + 2(1-p)]^2 + \sin^2\theta
\end{aligned}$$

□

**Lemma 3.** For any  $j \in [1, k]$ ,  $C_j = \mathcal{Q}^{\frac{3^j-1}{2}} C$ .

*Proof.* We will give a quick sketch of the proof by induction.

For  $k=1$ ,  $C_1 = G_\epsilon^* = CS_{|\psi\rangle}C^\dagger S_{\mathcal{P}}C = \mathcal{Q}C$  so the claim holds for the base case.

Now, suppose that the claim holds for some  $1 \leq j < k$ . Before discussing the induction case, note that  $(\mathcal{Q}^\dagger)^t = (S_{\mathcal{P}}CS_{|\psi\rangle}C^\dagger)^t = S_{\mathcal{P}} \cdot \mathcal{Q}^{t-1} \cdot (CS_{|\psi\rangle}C^\dagger)$  for any  $t$ .

Then,  $C_{j+1} = G_{\epsilon_j}^*(C_j, |\psi\rangle, \mathcal{P}) = C_j S_{|\psi\rangle} C_j^\dagger S_{\mathcal{P}} C_j$  which, using the induction hypothesis, is  $\mathcal{Q}^{(3^j-1)/2} C$ .  
 $S_{|\psi\rangle} \cdot C^\dagger (\mathcal{Q}^\dagger)^{(3^j-1)/2} \cdot S_{\mathcal{P}} \mathcal{Q}^{(3^j-1)/2} C =$  (using the expression for  $(\mathcal{Q}^\dagger)^t$  above)  $\mathcal{Q}^{(3^j-1)/2+1+(3^j-1)/2-1+1+(3^j-1)/2} C = \mathcal{Q}^{(3^{j+1}-1)/2} C$ . □

## C Optimum initial state for distinguishing two circuits

Recall that  $|\langle\psi_1|\psi_2\rangle| = |\langle\phi|C_1^\dagger C_2|\phi\rangle|$ . Denoting  $C_1^\dagger C_2$  by  $S$ , we would like to minimize  $|\langle\phi|S|\phi\rangle|$  over all possible pure state  $|\phi\rangle$ . Suppose the eigenvalues of  $S$  are  $e^{i\theta_1}, \dots$  with corresponding eigenvectors  $|v_1\rangle, \dots$ . Using a recent result [2], the maximum value of  $\epsilon$  is obtained by solving the optimization problem

$$\min f(\theta_1, \dots) = \left( \sum_j c_j^2 + \sum_{j \neq k} c_j c_k \cos(\theta_j - \theta_k) \right), \quad \text{where, } \sum_j c_j = 1, \quad 0 \leq c_j \leq 1$$

Suppose  $f_{OPT}$  denotes the optimal value above and  $c_1, \dots$  denote the corresponding solution. Then, the optimal  $\epsilon$  is  $1 - f_{OPT}^2$  and  $|\phi\rangle$  can be set to  $\sum_j \sqrt{c_j} |v_j\rangle$ .